القسم السابع: نطاق العمل المفصل

٦٠ نطاق عمل المشروع

- **حل الالتزام والتدقيق للأمن السيبراني**

توريد حل لتوفير رؤية كاملة للشبكة عن طريق بناء تصور الشبكات المعقدة باستخدام خريطة الشبكة الديناميكية ليساعد في تعيين مجموعات قواعد جدار الحماية وتنظيفها وتحسينها وتحديد المخاطر والتخفيف من حدتها تحديد وفرض تجزئة الشبكة. يجب أن يقوم الحل تلقائيًا بسحب المعلومات من مجموعة كبيرة من الأجهزة لإنشاء خريطة هيكل شبكة تفاعلية للشبكة غير المتجانسة بالكامل. من خلال هذه الخريطة، لتمكين فهم تأثير سياسات أمان الشبكة على حركة المرور، واستكشاف مشكلات الاتصال بسرعة، وتخطيط التغييرات وتنفيذ استعلامات حركة المرور ويجب أن يدعم الحل المتوقع بتحديد أولوية للمخاطر.

محلل جدار الحماية يكتشف ويعطي الأولوية لجميع المخاطر والقواعد المرتبطة بها والتطبيقات المرتبطة بها في ملف سياسة أمان الشبكة. يجب أن يعتمد الحل المتوقع على قاعدة معرفة بالمخاطر والتي تشمل لوائح مبنية على أفضل الممارسات في مجال الأمن السيبراني ولابد أن يسهل من فرض تقسيم الشبكة (Micro segmentation) عبر الشبكة وعبر جميع أنظمة جداران الحماية لابد أن يقوم الحل إنشاء ملفات تقارير امتثال جاهزة للتدقيق ومعبأة مسبقًا لجميع أفضل الممارسات في مجال الأمن السيبراني على سبيل المثالا لا الحصر (NIST, DISA, STIGs, NCA, FISMA, ISO) لتقليل جهود إعداد التدقيق.

يجب أن يحتوي الحل على نظام لتطبيق سير وإجراءات العمل قابل للتعديل والتكيف بدرجة كبيرة لتبسيط وأتمتة عملية تغيير سياسة الأمان بأكملها، إبتداءاً من التخطيط والتصميم إلى تحليل المخاطر الاستباقي والتنفيذ على الجهاز والتحقق من الصحة والتدقيق. كجزء من عملية إدارة التغيير حيث يجب أن يقوم الحل بإغلاق أي طلبات تغيير غير ضرورية، مثل الطلبات التي تعمل بالفعل، مما يساعد على منع التغييرات الزائدة عن الحاجة ويراقب باستمرار جميع تغييرات على السياسة ليضمن ارتباطها بطلب مسبق معين، أو لاكتشاف ومنع التغيير الغير المصرح به، أو التغييرات الغريبة والغير عادية. يجب أن يتم توثيق كل خطوة في عملية التغيير بشكل كامل لمتابعة مستوى الإلتزام واتفاقيات مستوى الخدمة. بالإضافة إلى ذلك، يجب أن يوفر الحل مسار تدقيق كامل للمدققين (Auditors).

وللتأكد من العمليات التشغيلية وتحقيق مستهدفات الحل التقني لحلول الالتزام والتدقيق للأمن السيبراني يلتزم بتوفير الدعم المستمر خلال ساعات العمل الرسمي وذلك في مرحلة الدعم الفني مع مراعاة المؤهلات المطلوبة والموضحة بالشروط الخاصة لمدة (١٢) شهر حتى نهاية المشروع.

الامتثال

أ. تحسين قواعد جدار الحماية
ب. الاتساق في التدقيق والامتثال

الرؤية

أ. تصور خريطة الشبكة
ب. فرض مقترحات تجزئة الشبكة لحمايتها
ج. شهادة المطابقة الجاهزة مع أفضل الممارسات العالمية
د. الحفاظ على الرؤية المتمحورة حول التطبيق
ه. تقييم تأثير التغييرات على اتصال التطبيق والأمن والامتثال

الأتمتة الذكية

أ. أتمتة عملية التغيير

ب. التحقق من أن التغيير لا يترتب عليه مخاطر للشبكة
ج. التحقق من صحة تنفيذ تغييرات جدار الحماية لتوفير الوقت

- **حل التحقق من صحة التحكم الأمني**

توفير منصة تحتوي مجموعة من الميزات التقنية من أجل التقييم تلقائيا والإبلاغ عن الاحداث الأمنية في الوقت الفعلي وتوفير مستوى الحماية ضد التهديدات التي توفرها الضوابط الأمنية من خلال محاكاة الهجمات الإلكترونية.

عندما يتم العثور على ثغرات أمنية تتطلب إجراءات تخفيف حالية ومعروفة وفقا لضــوابط الأمان المتاحة، يتعين على المنصـــة تقديم تقرير عن الضوابط والاشادة بالحلول.

الإبلاغ عن مستوى الكفاءة في الكشف عن حوادث أمن المعلومات، والتي تقاس بصـحة الحوادث ضـمن عينة معينة والتي يتم تسليط الضـــوء عليها من خلال البنية التحتية لأمن تكنولوجيا المعلومات، و / أو التأخير بين وقوع الحادث وتوليد الأحداث الأمنية ذات الصلة.

في حالة وقوع حوادث غير مكتشفة والتي قد يتم اكتشافها بدلا من ذلك وفقا لأنظمة الكشف عن نقطة النهاية الحالية والقدرات الحالية لأنظمة إدارة أحداث المعلومات، فإن النظام الأساسي هو تقديم الحلول المناسبة للكشف عن التهديدات.

وللتأكد من العمليات التشـغيلية وتحقيق مسـتهدفات الحل التقني لحلول التحقق من صـحة التحكم الأمني يلتزم بتوفير الدعم المسـتمر خلال سـاعات العمل الرسـمي وذلك في مرحلة الدعم الفني مع مراعاة المؤهلات المطلوبة والموضـحة بالشروط الخاصـة لمدة (١٢) شهر حتى نهاية المشروع.

- **حل أمن البريد الالكتروني**

توفير حل لحماية الوثائق التي تدار في أنظمة وزارة الدفاع، والتي تكون خالية من الوصـول غير المصـرح به وتخضـع دائما للتحكم، بغض النظر عما إذا كانت هذه الوثائق على البنية التحتية الداخلية لوزارة الدفاع، كما لو تمت مشـــاركتها مع مســـتخدمين آخرين في وزارة الدفاع أو موقع آخر أو مع أجهزة أو معدات غير خاضـــعة للرقابة حيث يجب أن يحتوي الحل المقدم على الخصــــائص التالية على الأقل، لضمان قابليته للاستخدام ووظائفه في بيئة العميل:

أ. التصـــميم: يجب أن يكون الحل قابلا للتثبيت محليا بنســبة ١٠٠٪ دون أي تفاعل مع ســحابة خارجية أو بنية تحتية خارجية ويجب أن يكون قابلا للتثبيت على أنظمة Linux الأساسية.
ب. إنفاذ الأذونات اجباريا وضــوابط الوصــول إلى الوثائق: تطبيق الأذونات والقيود على الوثائق وفقا لنوع ســرية الملف. حيث يتمكن المســتخدم من تطبيق الأذونات التالية على الملف: العرض والتحرير والطباعة والنسـخ واللصـق، وإمكانية إضـــافة مستخدمين تابعين لجهات خارجية أو التحكم الكامل في الملف لحمايته.
ج. الحماية الديناميكية وإمكانية إلغاء الوصول إلى الوثائق: يجب أن يكون من الممكن حماية المستخدمين الفرديين (الداخليين أو الخارجيين) ومجموعات مستخدمي Active Directory وحتى المجالات بأكملها عن طريق تشفير المستندات.
د. إدارة الهوية: يجب أن يكون الحل قادرًا على التكامل مع AD/LDAP أو أي مســتودع للمســـتخدمين ويجب أن يكون من الممكن العمل مع أدوات إدارة الهوية أو أدوات إدارة حساب الامتياز من خلال التكامل مع .AD
ه. التدقيق وتتبع الوثائق المحمية: يجب أن يكون المستخدم المسؤول قادرا على الوصـول إلى تدقيق جميع المستندات المحمية في وزارة الدفاع، وتصور كل من عمليات الوصول المصرح بها ومحاولات الوصول غير المصرح بها، بالإضافة إلى أي إجراء إلغاء حماية قد يكون تم إجراؤه.
و. مشاركة المعلومات المحمية مع المستخدمين الداخليين والخارجيين: يجب أن يكون الحل متوافقًا مع أي إصدار من Office بدءًا من Office 2010 وما بعده .يجب ألا يحتاج المســـتخدمون إلى تثبيت أي برامج أو تطبيقات إضــــافية لفتح البيانات المحمية .ينبغي دعم الأنظمة الأسـاسـية Windows و Mac OSXو iOSوAndroid، ويجب أن تكون العلامة المائية متاحة عند فتح البيانات عبر الويب للوصـــول بدون وكيل، وعلى الأجهزة المحمولة التي تســـتخدم تطبيق الهاتف المحمول، وعلى التطبيقات الأصلية لأجهزة Windows و.Mac OS
ز. الوصول والحماية بدون وكيل (Agentless) : يجب أن يوفر الحل وسيلة للوصول إلى البيانات المحمية مثل ملفات MS Officeوملفات PDF والصور ورسائل البريد الإلكتروني، وحتى تحريرها (إذا تم منحهم الإذن للقيام بذلك)، من أي نظام أساسي (Windows و Macو .(Linuxومن أي متصفح، دون الحاجة إلى تثبيت أي وكيل أو تثبيت مجموعة Office أو قارئ.PDF
ح. العلامات المائية والضوابط الأخرى على الوثائق المحمية: يجب أن تكون العلامة المائية الديناميكية قابلة للتطبيق على جميع المستندات المحمية) ملفات MS Office وملفات PDF والصور وما إلى ذلك (ورسائل البريد الإلكتروني، لتخفيف لقطات



الشـــاشـــة وزيادة التحكم في المعلومات الحســـاســـة .يجب أن تكون العلامة المائية قابلة للتطبيق على نظامي التشـــغيل Windowsو MAC، والوصـول عبر الإنترنت من متصـفحات الويب المدعومة، وعلى الأجهزة المحمولة Android و.(IOS

ط. إدارة السياسة الديناميكية من قبل المستخدمين والمسؤولين: يجب أن يكون المسؤول قادرًا على إنشاء سياسات مرئية فقط لأشخاص أو مجموعات معينة .يمكن منح الأذونات لمجموعات Active Directory والمستخدمين الداخليين والمستخدمين الخارجيين .يمكن تعيين مسؤولين مفوضين لحماية البيانات مسؤولين عن المجموعات والأقسام.

ي. حماية البريد الإلكتروني: حماية جميع المستخدمين والحد من الأذونات التي يمكن منح الوصول إليها، بالإضـافة إلى تحديد تواريخ انتهاء الصلاحية للمعلومات المرسلة .ليس من الضروري أن يكون لديك Outlook للوصول إلى النص الأساسي أو المرفقات المحمية.

ك. تصنيف البيانات: يجب أن يتضمن الحل تصنيف للبيانات لدعم البنية التحتية الأمنية لدينا .يجب أن تشمل الوظائف الرئيسية إمكانيات التصنيف المقترحة واليدوية، مما يمكّن المستخدمين من تصنيف البيانات بناءً على سياسات ومستويات حساسية محددة مسبقًا.

ل. التكامل مع AD : يجب أن يكون الحل قادرًا على العمل مع تكامل AD ويمكن اســـتخدام بيانات اعتماد المجال لتســـجيل الدخول (الدخول الموحد) والســـماح بالحماية للمجموعات المحددة في AD بدلاً من المســـتخدمين الفرديين .يجب أن يدعم الدلائل النشطة في مجموعة التفرعات المختلفة.

م. التكامل مع الأنظمة الأمنية: يجب أن يكون الحل المقدم قادرًا على التكامل مع الأنظمة الأمنية مثل الـ SIEM ، بحيث يمكن الوصـــول إلى الأحداث إلى المســـتندات المحمية والتنبيهات المتعلقة بها ومحاولات الوصـــول بدون أذونات وإلغاء حماية المستندات وما إلى ذلك

ن. الإدارة المركزية: ســـتكون وحدة التحكم الإدارية متاحة لمراقبة النشـــاط (الحماية، والوصـــول، والتنبيهات، وما إلى ذلك) للمستندات المحمية الخاصة بوزارة الدفاع يمكن إجراء التتبع في الوقت الفعلي، مما يسمح برؤية المستندات التي تم الوصول إليها بواسطة مستخدم معين أو المستخدمين الذين وصلوا إلى مستند معين .يجب أن يكون من الممكن أيضًا عرض تقارير حول التنبيهات المتعلقة بالوصول إلى المستندات، والرسوم البيانية الموجزة، وما إلى ذلك، مما يسمح برؤية كاملة لما يحدث مع وثائق المنظمة .يجب أن يكون حامي البيانات أيضًـــا قادرًا على تلقي تقرير يومي عن جميع الأنشـــطة التي تحدث على البيانات .يمكن للمسؤول إنشاء سياسات حماية وتعيينها للمستخدمين ومجموعات المستخدمين والأقسام وما إلى ذلك، بحيث يكون المستخدمون متاحين لحماية المستندات بتصنيف الحماية الذي يريدونه، دون الحاجة إلى إنشائها بأنفسهم .يمكنك أيضًا تعديل سـياسـات المسـتخدم .يمكن للمسـؤول إدارة المسـتخدمين الداخليين والخارجيين من لوحة التحكم .سـيكون قادرًا على رؤية المسـتخدمين المسجلين في Active Directory ، وأولئك الذين تم توفيرهم تلقائيًا بعد تضـمينهم في السياسـة، وما إلى ذلك .يمكن للمسؤول نقل ملكية المستندات المحمية بين المستخدمين .ويمكن القيام بذلك لجميع المستندات أو عن طريق سياسة الحماية .ولكن لا يجوز له نقل الملكية لنفسه .وذلك لتجنب وجود مستخدم متميز يمكنه الوصول إلى جميع المستندات.

وللتأكد من العمليات التشـغيلية وتحقيق مسـتهدفات الحل التقني لحلول أمن البريد الإلكتروني يلتزم بتوفير الدعم المسـتمر خلال سـاعات العمل الرسـمي وذلك في مرحلة الدعم الفني مع مراعاة المؤهلات المطلوبة والموضـحة بالشـروط الخاصـة لمدة (١٢) شهر حتى نهاية المشروع.

- **حل أمن الشبكة (NDR)**

توفير حل مراقبة الشبكة الداخلية (NDR) لشبكة قوات الدفاع الجوي وكشف التهديدات في الشبكة والأنشطة الضارة والاستجابة لها بالإمكانيات الكامنة بالحل أو من خلال التكامل.

يشمل نطاق العمل بشكل إجمالي:

أ. توريد وتثبيت نظام كشـف التهديدات والانشـطة الضـارة بالشـبكة (NDR) وتطبيق كافة ما ذكر في بند المواصـفات الفنية التفصيلية. بالملحق رقم (٢).
ب. توريد الرخص.
ج. تقديم الدعم الفني للرخص المقدمة لمدة ثلاث سنوات للمشروع.
د. توثيق وتجميع تفاصيل تنفيذ المشروع.
ه. اختبار إعدادات الخدمات المقدمة في المشروع.



و. يجب الالتزام باتفاقية مستوى الخدمة (SLA).
ز. على الشركة توريد وبرمجة النظام على أعلى معايير أمنية على سبيل المثال لا الحصر (NIST, DISA, STIGs, NCA, FISMA, ISO)
ح. تلتزم الشركة بتقديم ما يثبت أنها مورد أو موزع معتمد لدى وكيل الشركة الصانعة في المملكة العربية السعودية.
ط. ضمان شامل على جميع البرامج ويشمل الصيانة والدعم طوال مدة العقد لمدة (٣٠) شهر.
ي. تلتزم الشركة بتقديم CD يحتوي على المواصفات الفنية كما هي من الشركة المصنعة.
ك. تلتزم الشركة بتقديم خطة عمل للتوريد والتركيب ويتم تقديم تقارير أسبوعية أثناء مدة العمل.
ل. توريد وتثبيت نظام كشف التهديدات والانشطة الضارة بالشبكة (NDR) وتطبيق كافة ما ذكر في بند المواصفات الفنية التفصيلية.
م. توريد رخص نظام كشف التهديدات والأنشطة الضارة بالشبكة.
ن. تقديم الدعم الفني للرخص المقدمة في تنفيذ مجال العمل طوال مدة العقد لمدة (٣٠) شهر.
س. اختبار إعدادات الخدمات المقدمة في المشروع.

- **نقل المعرفة**

نقل معرفة أفضل الممارسات في الأمن السيبراني، وإجراء نقل المعرفة وتوفير إجراءات التشغيلية في وزارة الدفاع داخل مدينة الرياض.

يجب أن يقوم المقاول بتقديم خطة ومنهجية واضحة لتنفيذ نقل المعرفة تتضمن عدد (٥) ورش عمل وبحد أدنى (١٠) مقعد وان لا تقل عن (٥) أيام لكل ورشة عمل لدى إدارة الأمن السيبراني بالشؤون التنفيذية، ويتم تقديم هذه الخطة مع العرض الفني.

يمكن للمقاول تقديم منهجية نقل المعرفة التي يراها مناسبة التي تضمن أن يستطيع منسوبو الوزارة من استخدام الأنظمة داخل نطاق عمل المشروع، وتشمل متطلبات نقل المعرفة بما يشمل الإطار العام لنقل المعرفة لمنسوبي الوزارة من استخدام الأنظمة المطورة وفق البنود المذكورة في جدول الكميات.

- **الدعم الفني**
  - تبدأ هذه المرحلة بعد إنجاز جميع المراحل السابقة وقبولها وتمتد طوال مدة الدعم والصيانة لمدة ١٢ شهر، وتشمل أعمال الصيانة والدعم على جميع ما تم ذكره في نطاق عمل المشروع، والقيام خلالها بتطوير وتنفيذ خطة نقل المعرفة التقنية للمختصين الفنيين بالوزارة ودعمهم حتى يتمكنوا من استلام الأنظمة بعد انتهاء الفترة المحددة.
  - يلتزم المقاول بتكليف المهندسين والفنيين المتخصصين لديهم للدعم الفني للأجهزة الموردة للوزارة ، وتلتزم الشركة بإشراك الفنيين من منسوبي الإدارة العامة لتقنية المعلومات في جميع أعمال الصيانة والدعم الفني التي يقومون بها وتعريفهم على أنواع الأعطال الفنية ومسبباتها والطرق الصحيحة لمعالجتها وإصلاحها.
  - يلتزم المقاول بتكليف وتواجد مهندس مقيم لكل حل من الحلول الموضحة في مجال العمل في أوقات العمل الرسمية في الوزارة وذلك خلال فترة الدعم الفني.
  - تقديم المؤهلات الفنية لمهندسي الدعم الفني ضمن فريق عمل تنفيذ المشروع.
  - يلتزم المقاول بتزويد الإدارة العامة لتقنية المعلومات ببيانات (هاتف – بريد- جوال- فاكس ...) مركز اتصال بالشركة لطلب الصيانة أو اصلاح مشكلة في النظام.
  - أن تكون تلبية طلبات الصيانة العادية خلال ٤٠ ساعة بحد أقصى ، والصيانة الطارئة خلال ١٦ ساعات بحد أقصى.
  - الصيانة العادية هي الصيانة لأجهزة وبرامج الوزارة التي لا تؤثر على سير عمل الوزارة وتكون خلال ساعات العمل.
  - يلتزم المقاول بتزويد الجهة المستفيدة (هاتف – بريد- جوال- فاكس ...) مركز اتصال بالشركة لطلب الصيانة أو اصلاح مشكلة في النظام.

تصنيف الحدث	مدة الاستجابة	وقت الحل
حرج	١ ساعة	٢ ساعة عمل
متوسط	٢ ساعة	٤ ساعات عمل



منخفض	٤ ساعات	١٦ ساعة عمل

- **الضمان**
  - يجب على المقاول توفير فترة **ضـــمان لمدة (٢)** ســـنوات بعد انتهاء مدة العقد لجميع البرامج المقدمة والأجهزة والخدمات المثبتة بموجب العقد، يخضع لنظام الوكالات التجارية.

٦١ برنامج العمل

الجدول الزمني		
	مراحل العقد	**الفترة الزمنية**
١	مدة التنفيذ المشروع	١٨ شهر
٢	الدعم الفني	١٢ شهر
٣	مدة العقد كاملة	٣٠ شهر

ت	بداية الفترة **Start**	نهاية الفترة **End**	المهام / الأنشطة **Task/ Activities Description for Project**
١	**T0**	**T0**	بداية توقيع العقد Starting of Project
٢	**T0**	**T0 + 1 month**	مسح ميداني للموقع Survey of Project Sites
٣	**T0 + 1 month**	**T0 + 2 month**	تقديم خطة العمل لبنود العقد للطرف الأول والموافقة عليها Delivery of Survey Reports and Project Design of Project for approval.
٤	**T0 + 2 month**	**T0 + 15 month**	تنفيذ بنود المشروع (توريد وتركيب الأنظمة بالشبكة وتأمين الرخص والدعم الفني) Completion of Installation of Project.
٥	**T0 + 15 month**	**T0 + 18 month**	تسليم ملف المشروع النهائي Delivery of Project Files



٦	**T0 + 18 month**	**T0 + 18 month**	القبول والاستلام والنهائي Completion of Acceptance and Signing of "Certificate of Acceptance of Project"
7	**T0 + 18 month**	**T0 + 30 month**	الدعم الفني

تعتبر الفترة الزمنية والترتيب الزمني للمبادرات والأنشطة الرئيسية الموضحة أدناه **بمثابة دليل توجيهي**، إذ تم الوصول إليها اعتمادا على خارطة الطريق للتنفيذ التي تم وضـعها لكامل عملية التطوير -وبناءً على اعتبارات أخرى -لضـمان تماشـيها مع التداخلات بين المبادرات الحالية، قد يقترح الموردون في عروضــهم المقدمة بعض التعديلات على الجدول الزمني وتسلسـل الأنشـطة وفقًا لنهجهم المقترح وخبرتهم السابقة في تنفيذ مشاريع مشابهة، وتنفيذ بعض الأنشطة الرئيسة بالتزامن ، دون تجاوز الفترة الزمنية الكلية المحددة لكل مرحلة من مراحل المشروع.
يجب على المقاول الإلتزام بالبنود التالية:

- الشروع في بدا المشروع من تاريخ استلام الموقع بموجب محضر الاستلام.
- الشروع بإستكمال تسكين الموظفين في غضون ٢ أسبوعًا من إصدار **"**إشعار استلام الموقع**"**.
- تطوير خطة تفصـيلية توضـح كيفية التنفيذ والجدول الزمني وورش العمل اللازمة للتأكد من التنفيذ السـلس عبر جميع فرق وزارة الدفاع
- يجب على المقاول مراجعة خطة التنفيذ مع وزارة الدفاع، والحصول على الموافقة الصحيحة قبل الشروع في الخطة
- يجب على المقاول اتباع الأولويات التي حددتها وزارة الدفاع للتنفيذ

- **الأنشطة**

أ. تجهيز البنية التحتية لتركيب الأنظمة في مركز البيانات
ب. تجهيز أجهزة الشـبكة المراد ربطها مع الحل وتخصـيص الصـلاحيات المطلوبة لعناصـر الشـبكة واسـم المسـتخدم المراد استخدامه
ج. التأكد من أن جميع صلاحيات الشبكة متوفرة بين الحل والأجهزة المراد ربطها بالنظام
د. ربط الأجهزة مع الحل
ه. تحليل الأجهزة المرتبطة بالحل
و. تطوير خريطة الشبكة من الأجهزة المرتبطة بالحل
ز. تخصيص طلبات التغيير في الحل
ح. تعيين الأشخاص المسؤولين عن إجراءات التغيير والموافقة عليها
ط. مراجعة عملية التركيب والتشغيل
ي. إتمام الاختبارات التشغيلية (UAT)والأمنية (PT) .
ك. نقل المعرفة

٦٢ مكان تنفيذ الأعمال

سـيتم إقامة المشـروع وتوريد وتشـغيل الانظمة وملحقاتها وبرامجها التشـغيلية والبرامج التطبيقية وقواعد البيانات والخوادم وتوفير الخدمات المضمنة بالكراسة في مواقع وزارة الدفاع بمدينة الرياض.

- مكان التوريد: مركز خدمات الانترنت بالإدارة العامة لتقنية المعلومات بالرياض.